Asymptotics of Quantum Relative Entropy From Representation Theoretical Viewpoint

Masahito Hayashi
Department of Mathematics, Kyoto University, Kyoto 606-8502, Japan
e-mail address: masahito@kusm.kyoto-u.ac.jp

Abstract

In this paper it was proved that the quantum relative entropy $D(\sigma\|\rho)$ can be asymptotically attained by Kullback Leibler divergences of probabilities given by a certain sequence of POVMs. The sequence of POVMs depends on ρ, but is independent of the choice of σ.

1 Introduction

In classical statistical theory the relative entropy $D(p\|q)$ is an information quantity which means the statistical efficiency in order to distinguish a probability measure p of a measurable space from another probability measure q of the same measurable space. The states correspond to measures on measurable space. When p, q are discrete probabilities, the relative entropy (called also information divergence) introduced by Kullback and Leibler is defined by [1]:

$$D(p\|q) := \sum_i p_i \log \frac{p_i}{q_i}.$$

In this paper, we consider the quantum mechanical case. Let $\mathcal{H}$ be a separable Hilbert space which corresponds to the physical system of interest. In quantum theory the states of a system correspond to positive operators of trace one on $\mathcal{H}$. (These operators are called densities.) The quantum relative entropy of a state ρ with respect to another state σ is defined by [2]:

$$D(\sigma\|\rho) := \mathrm{Tr}[\sigma(\log\sigma - \log\rho)].$$

States are distinguished through the result of a quantum measurement on the system. The most general description of a quantum measurement probability is given by the mathematical concept of a *positive operator valued measure* (POVM) $M = \{M_i\}_{i=1}^{h(M)}$ [3, 4] which is a partition of the unit $\mathrm{Id}_{\mathcal{H}}$ such that any M_i is nonnegative operator. A POVM $M = \{M_i\}$ on $\mathcal{H}$ is called *Projection Valued Measure* (PVM), if any M_i is projection. In quantum mechanics, $P^M_\rho(i) = \mathrm{Tr}[M_i\rho]$ describes the probability distribution given by a POVM M with respect to a state ρ. Then we define the quantity $D_M(\sigma\|\rho)$ as [2]:

$$D_M(\sigma\|\rho) := D(P^M_\sigma\|P^M_\rho).$$

Thus an information quantity we can directly access by a measurement M is not $D(\sigma\|\rho)$ but $D(P^M_\sigma\|P^M_\rho)$. The map $\rho \mapsto P^M_\rho$ is the dual of a unitpreserving completely positive map. Therefore, we have the following by Uhlmann inequality [5]:

$$D_M(\sigma\|\rho) \le D(\sigma\|\rho). \tag{1}$$

The equality is attained by a certain POVM M when and only when $\rho\sigma = \sigma\rho$.

In this paper, we consider asymptotic attainment of the equality of the inequality (1). In order to answer the question we define the quantum i.i.d.-condition which is the quantum analogue of the independent and identically distribution condition. If there exist n samples of the state ρ, the quantum state is described by $\rho^{\otimes n}$ defined by:

$$\rho^{\otimes n} := \underbrace{\rho \otimes \cdots \otimes \rho}_{n} \text{ on } \mathcal{H}^{\otimes n},$$

where the composite system $\mathcal{H}^{\otimes n}$ is defined as:

$$\mathcal{H}^{\otimes n} := \underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n}.$$

In this paper, we call this condition the quantum i.i.d.-condition. Related to the inequality (1), it is well-known that $D(\sigma^{\otimes n}\|\rho^{\otimes n}) = nD(\sigma\|\rho)$.

Let M_n be a POVM on $\mathcal{H}^{\otimes n}$, then we have

$$\frac{1}{n} D_{M_n}(\rho^{\otimes n}\|\sigma^{\otimes n}) \leq D(\sigma\|\rho). \tag{2}$$

Therefore, we consider the attainment of the equality of (2) in taking the limit of $n \to \infty$. Hiai and Petz[7] proved the following theorem with respect to this problem.

Theorem 1 *Assume that the dimension of $\mathcal{H}$ is finite. Let σ_n be a state on $\mathcal{H}^{\otimes n}$. If the sequence $\{\frac{1}{n}D(\sigma_n\|\rho^{\otimes n})\}$ convergence as $n \to \infty$, then we have*

$$\lim_{n\to\infty} \frac{1}{n} D(\mathcal{E}_{\rho^{\otimes n}}(\sigma_n)\|\rho^{\otimes n}) = \lim_{n\to\infty} \frac{1}{n} D(\sigma_n\|\rho^{\otimes n}), \tag{3}$$

where $\mathcal{E}_{\rho^{\otimes n}}$ denotes the conditional expectation defined in (6) in the following section.

The preceding theorem implies that

$$\lim_{n\to\infty} \frac{1}{n} D_{E(\mathcal{E}_{\rho^{\otimes n}}(\sigma_n))\times E(\rho^{\otimes n})}(\sigma_n\|\rho^{\otimes n}) = \lim_{n\to\infty} \frac{1}{n} D(\sigma_n\|\rho^{\otimes n}),$$

where the PVM $E(\mathcal{E}_{\rho^{\otimes n}}(\sigma_n)) \times E(\rho^{\otimes n})$ is defined in the following section. In this paper, we consider whether a sequence of PVMs satisfying (4) depends on σ_n in the case of that the state σ_n satisfies the quantum i.i.d.-condition i.e. $\sigma_n = \sigma^{\otimes n}$:

$$\frac{D_{M_n}(\sigma^{\otimes n}\|\rho^{\otimes n})}{n} \to D(\sigma\|\rho) \text{ as } n \to \infty \ \forall \sigma. \tag{4}$$

We will consider this problem from a representation theoretical viewpoint. The main theorem of this paper is the following theorem.

Theorem 2 *Let ρ be a state on $\mathcal{H}$, then there exists a sequence $\{(l_n, M_n)\}$ of pairs of an integer and a measurement on $\mathcal{H}^{\otimes l_n}$ such that*

$$\frac{D_{M_n}(\sigma^{\otimes l_n}\|\rho^{\otimes l_n})}{l_n} \to D(\sigma\|\rho) \text{ as } n \to \infty \ \forall \sigma. \tag{5}$$

In the finite-dimensional case, the convergence of (5) is uniform for all σ.

2 Preliminary

Next, we consider the relation between a PVM and a quantum relative entropy. We put some definitions for this purpose. A state ρ is called *commutative* with a PVM $E(=\{E_i\})$ on $\mathcal{H}$ if $\rho E_i = E_i \rho$ for any i. For PVMs $E(=\{E_i\}), F(=\{F_j\})$, we denote $E \le F$ if for any i there exist subsets $\{(F/E)_i\}$ such that $E_i = \sum_{j \in (F/E)_i} F_j$. For a state ρ, $E(\rho)$ denotes the spectral measure of ρ which can be regarded a PVM. The *conditional expectation* $\mathcal{E}_E$ with respect to a PVM E is defined as:

$$\mathcal{E}_E : \rho \mapsto \sum_i E_i \rho E_i. \tag{6}$$

Therefore, the conditional expectation $\mathcal{E}_E$ is an affine map from the set of states to themselves. Then, the state $\mathcal{E}_E(\rho)$ is commutative with a PVM E. For simplicity, we denote the conditional expectation $\mathcal{E}_{E(\rho)}$ by $\mathcal{E}_\rho$.

Theorem 3 *Let E be a PVM such that $w(E) := \sup_i \dim E_i < \infty$. If states ρ, σ are commutative with a PVM E and a PVM F satisfies that $E, E(\rho) \le F$, then we have*

$$D_F(\sigma\|\rho) \le D(\sigma\|\rho) \le D_F(\sigma\|\rho) + \log w(E).$$

Note that there exists a PVM F such that $E, E(\rho) \le F$.
Proof It is proved by Lemma 1 and Lemma 2. □

Lemma 1 *Let σ, ρ be states. If a PVM F satisfies that $E(\rho) \le F$, then*

$$D(\sigma\|\rho) = D_F(\sigma\|\rho) + D(\sigma\|\mathcal{E}_F(\sigma)). \tag{7}$$

Proof Since $E(\rho) \le F$, F is commutative with ρ, we have $\operatorname{Tr} \mathcal{E}_F(\sigma) \log \rho = \operatorname{Tr} \sigma \log \rho$. Remark that $\operatorname{Tr} \mathcal{E}_F(\sigma) \log \sigma = \operatorname{Tr} \sigma \log \sigma$. Therefore, we get the following:

$$\begin{aligned} D_F(\sigma\|\rho) - D(\sigma\|\rho) &= \operatorname{Tr} \mathcal{E}_F(\sigma)(\log \mathcal{E}_F(\sigma) - \log \rho) - \operatorname{Tr} \sigma(\log \sigma - \log \rho) \\ &= \operatorname{Tr} \mathcal{E}_F(\sigma)(\log \mathcal{E}_F(\sigma) - \log \sigma). \end{aligned}$$

We get (7). □

Lemma 2 *Let E, F be PVMs such that $E \le F$. If a state σ is commutative with E, then we have*

$$D(\sigma\|\mathcal{E}_F(\sigma)) \le \log w(E). \tag{8}$$

Proof Let $a_i := \operatorname{Tr} E_i \sigma E_i, \sigma_i := \frac{1}{a_i} E_i \sigma E_i$, then $\sigma = \sum_i a_i \sigma_i$, $\mathcal{E}_F(\sigma) = \sum_i a_i \mathcal{E}_F(\sigma_i)$. Therefore,

$$\begin{aligned} & D(\sigma\|\mathcal{E}_F(\sigma)) = \sum_i a_i D(\sigma_i\|\mathcal{E}_F(\sigma_i)) \le \sup_i D(\sigma_i\|\mathcal{E}_F(\sigma_i)) \\ = & \sup_i (\operatorname{Tr} \sigma_i \log \sigma_i - \operatorname{Tr} \mathcal{E}_F(\sigma_i) \log \mathcal{E}_F(\sigma_i)) \\ \le & -\sup_i \operatorname{Tr} \mathcal{E}_F(\sigma_i) \log \mathcal{E}_F(\sigma_i) \le \sup_i \log \dim E_i = \log w(E). \end{aligned}$$

Thus, we get (8) □
If a PVM $F = \{F_j\}$ is commutative with a PVM $E = \{E_i\}$, then we can define the PVM $F \times E = \{F_j E_i\}$. Then we have $F \times E \ge E, F$. If E' is commutative with E, F and $F \ge E$, then we have $E' \times F \ge E' \times E$. If $F \ge E$ and $\frac{\operatorname{Tr}[F_j \rho]}{\operatorname{Tr}[E_i \rho]} = \frac{\operatorname{Tr}[F_j \sigma]}{\operatorname{Tr}[E_i \sigma]}$ for $j \in (F/E)_i$, then we have $D_F(\sigma\|\rho) = D_E(\sigma\|\rho)$.

3 Quantum i.i.d. condition from group theoretical viewpoint

From the orthogonal direct sum decomposition $\mathcal{H} = \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_k$, we can naturally constitute the PVM $\{P_{\mathcal{H}_i}\}$, where $P_{\mathcal{H}_i}$ denotes the projection of $\mathcal{H}_i$. In the following, we consider the relation between irreducible representations and PVMs.

3.1 group representation and its irreducible decomposition

Let V be a finite dimensional vector space over the complex numbers $\mathbb{C}$. A map π from a group G to the generalized linear group of a vector space V is called a *representation* if the map π is homomorphism i.e. $\pi(g_1)\pi(g_2) = \pi(g_1 g_2),\ \forall g_1, g_2 \in G$. For a subspace W of V, it is *invariant* with respect to a representation π if $\pi|_W(g_1)\pi|_W(g_2) = \pi|_W(g_1 g_2),\ \forall g_1, g_2 \in G$, where $\pi|_W$ denotes the restriction of π to W. In this case, $\pi|_W$ is called a *subrepresentation* of π. Let π be a representation to V, then π is called *irreducible* if there no proper nonzero invariant subspace of V. Let $\pi_1(\pi_2)$ be representations of a group G on $V_1(V_2)$ respectively. The *tensored* representation $\pi_1 \otimes \pi_2$ of G on $V_1 \otimes V_2$ is defined as: $(\pi_1 \otimes \pi_2)(g) = \pi_1(g) \otimes \pi_2(g)$, and the *direct sum* representation $\pi_1 \oplus \pi_2$ of G on $V_1 \oplus V_2$ is also defined as: $(\pi_1 \oplus \pi_2)(g) = \pi_1(g) \oplus \pi_2(g)$. If there is a invertible linear map f from V_1 to V_2 such that $f\pi_1(g) = \pi_2(g)f$, π_1 is *equivalent* with π_2. If W is an invariant subspace for a representation π on V , then there is a complementary invariant subspace W' for a representation π, so that $V = W \oplus W'$ and $\pi = \pi|_W \oplus \pi|_{W'}$. Therefore, any representation is a direct sum representation of irreducible representations.

Let π_1 (π_2) be a representation of W_1 (W_2) respectively. $W_1 \oplus W_2$ gives an irreducible decomposition of the direct sum representation $\pi := \pi_1 \oplus \pi_2$. If π_1 is equivalent with π_2, there is another irreducible decomposition. For example, there is an irreducible decomposition $\{v \oplus f(v) | v \in W_1\} \oplus \{v \oplus -f(v) | v \in W_1\}$, where f is a map which gives the equivalence with π_1 and π_2. If π_1 isn't equivalent with π_2, there is no irreducible decomposition except $W_1 \oplus W_2$. A direct sum decomposition $W = W_1 \oplus \cdots \oplus W_s$ is called *isotypic* with respect to a representation π if it satisfies the following conditions: *every irreducible component of W_i with respect to a representation $\pi|_{W_i}$ is equivalent with each other. If $i \neq j$, then any irreducible component of W_i with respect to a representation $\pi|_{W_i}$ isn't equivalent with any irreducible component of W_j with respect to a representation $\pi|_{W_j}$.*

For a representation π of G, we can define the subrepresentation $\pi|^{G_1}$ of a subgroup G_1 of G by restricting a representation π to G_1. If the subrepresentation $\pi|^{G_1}$ is irreducible, then the representation π is irreducible. But, the converse isn't true. In this paper, we call a subgroup G_1 of G *unramified* if any subrepresentation $\pi|^G$ is irreducible when the representation π of G is irreducible.

3.2 Relation between a unitary representation and a PVM

Let $\mathcal{H}$ be a finite-dimensional Hilbert space. A representation π to a Hilbert space $\mathcal{H}$ is called *unitary* if $\pi(g)$ is a unitary matrix for any $g \in G$. If $\mathcal{H}_1$ is an invariant subspace of $\mathcal{H}$ with respect to a unitary representation π, the orthogonal space $\mathcal{H}_1$ of $\mathcal{H}_2$ is invariant with respect to a unitary representation π. Therefore, we have $\pi = \pi|_{\mathcal{H}_1} \oplus \pi|_{\mathcal{H}_2}$. A unitary representation π can be described by the orthogonal direct sum representation of irreducible representations

which are orthogonal with one another. We can regarded the direct sum decomposition as a PVM. Remark that without unitarity we cannot deduce the orthogonality. If there is a pair of irreducible component whose elements are equivalent with one another. Therefore, a corresponding PVM is not unique. In this paper, we denote the set of PVMs corresponding to an orthogonal irreducible decomposition by $\mathcal{M}(\pi)$.

Elements of the isotypic decomposition of a unitary representation π are orthogonal with one another. Thus, we can define a PVM $N(\pi)$ as the isotypic decomposition. We call a representation π of a group G *quasi-unitary* if there exist an unramified subgroup G_1 such that the subrepresentation $\pi|^{G_1}$ is unitary. For a quasi-unitary representation π, we define $N(\pi)$ ($\mathcal{M}(\pi)$) by $N(\pi|^{G_1})$ ($\mathcal{M}(\pi|^{G_1})$) respectively. We can show the uniqueness of them. For a unitary representation π and $g \in G$, $\pi(g)$ is commutative with a PVM $M \in \mathcal{M}(\pi)$ and a PVM $N(\pi)$. Concerning a quasi-unitary representation π, we can prove the same fact.

3.3 Relation between the tensored representation and PVMs

Let the dimension of the Hilbert space $\mathcal{H}$ is k. Irreducible representations of the special linear group $\mathrm{SL}(\mathcal{H})$ and the special unitary group $\mathrm{SU}(\mathcal{H})$ are classified by the highest weight. Thus, any irreducible representation of the special linear group $\mathrm{SL}(\mathcal{H})$ is irreducible under restricting to the special unitary group $\mathrm{SU}(\mathcal{H})$. The special unitary group $\mathrm{SU}(\mathcal{H})$ is unramified subgroup of the special linear group $\mathrm{SL}(\mathcal{H})$. Also, the special linear group $\mathrm{SL}(\mathcal{H})$ is unramified subgroup of the general linear group $\mathrm{GL}(\mathcal{H})$ since the general linear group $\mathrm{GL}(\mathcal{H})$ is described as the direct sum group $\mathrm{SL}(\mathcal{H}) \times U(1)$.

We denote the natural representation of the general linear group $\mathrm{GL}(\mathcal{H})$, the special linear group $\mathrm{SL}(\mathcal{H})$, the special unitary group $\mathrm{SU}(\mathcal{H})$ to $\mathcal{H}$ by $\pi_{\mathrm{GL}(\mathcal{H})}$, $\pi_{\mathrm{SL}(\mathcal{H})}$, $\pi_{\mathrm{SU}(\mathcal{H})}$, respectively. We consider representations $\pi_{\mathrm{GL}(\mathcal{H})}^{\otimes n} := ((\cdots(\pi_{\mathrm{GL}(\mathcal{H})} \otimes \pi_{\mathrm{GL}(\mathcal{H})})\cdots) \otimes \pi_{\mathrm{GL}(\mathcal{H})})$, $\pi_{\mathrm{SL}(\mathcal{H})}^{\otimes n} := ((\cdots(\pi_{\mathrm{SL}(\mathcal{H})} \otimes \pi_{\mathrm{SL}(\mathcal{H})})\cdots) \otimes \pi_{\mathrm{SL}(\mathcal{H})})$ and $\pi_{\mathrm{SU}(\mathcal{H})}^{\otimes n} := ((\cdots(\pi_{\mathrm{SU}(\mathcal{H})} \otimes \pi_{\mathrm{SU}(\mathcal{H})})\cdots) \otimes \pi_{\mathrm{SU}(\mathcal{H})})$ to the tensored $\mathcal{H}^{\otimes n}$. Remark that $\pi_{\mathrm{GL}(\mathcal{H})}^{\otimes n}|^{\mathrm{SL}(\mathcal{H})} = \pi_{\mathrm{SL}(\mathcal{H})}^{\otimes n}$, $\pi_{\mathrm{GL}(\mathcal{H})}^{\otimes n}|^{\mathrm{SU}(\mathcal{H})} = \pi_{\mathrm{SU}(\mathcal{H})}^{\otimes n}$. From the unitarity of the representation $\pi_{\mathrm{SU}(\mathcal{H})}^{\otimes n}$, representations $\pi_{\mathrm{GL}(\mathcal{H})}^{\otimes n}$ and $\pi_{\mathrm{SL}(\mathcal{H})}^{\otimes n}$ are quasi-unitary. Therefore, the set $\mathcal{M}(\pi_{\mathrm{SU}(\mathcal{H})}^{\otimes n})$ (the PVM $N(\pi_{\mathrm{SU}(\mathcal{H})}^{\otimes n})$) is consistent with the sets $\mathcal{M}(\pi_{\mathrm{SL}(\mathcal{H})}^{\otimes n}), \mathcal{M}(\pi_{\mathrm{GL}(\mathcal{H})}^{\otimes n})$ (the PVMs $N(\pi_{\mathrm{SL}(\mathcal{H})}^{\otimes n}), N(\pi_{\mathrm{GL}(\mathcal{H})}^{\otimes n})$) and we denote it by $Ir^{\otimes n}$ ($IR^{\otimes n}$) respectively.

From the Weyl's dimension formula ((7.1.8) or (7.1.17) in Goodman-Wallch[10]), The n-th symmetric space is the irreducible subspace in the representation $\pi_{\mathrm{GL}(\mathcal{H})}^{\otimes n}$ whose dimension is maximum. Its dimension is the repeated combination ${}_kH_n$ evaluated by ${}_kH_n = \binom{n+k-1}{k-1} = \binom{n+k-1}{n} = {}_{n+1}H_{k-1} \leq (n+1)^{k-1}$. For $M \in Ir^{\otimes n}$, we have the following:

$$w(M) \leq (n+1)^{k-1}. \tag{9}$$

Lemma 3 *Let σ be a state on $\mathcal{H}$. Then a PVM $M \in Ir^{\otimes n}$ and the PVM $IR^{\otimes n}$ is commutative with tensored state $\sigma^{\otimes n}$.*

Proof If $\sigma \in \mathrm{GL}(\mathcal{H})$, then this lemma is trivial. If $\sigma \notin \mathrm{GL}(\mathcal{H})$, there exists a sequence $\{\sigma_i\}_{i=1}^{\infty}$ of elements of $\mathrm{GL}(\mathcal{H})$ such that $\sigma_i \to \sigma$ as $i \to \infty$. Therefore we have $\sigma_i^{\otimes n} \to \sigma^{\otimes n}$ as $i \to \infty$. Because a PVM M is commutative with $\sigma_i^{\otimes n}$, the PVM M is commutative with $\sigma^{\otimes n}$. Similarly, we can prove that the PVM $IR^{\otimes n}$ is commutative with $\sigma^{\otimes n}$. □

From the definition of $Ir^{\otimes n}$ and $IR^{\otimes n}$, if $j \in (M/IR^{\otimes n})_i$, we have

$$\#(M/IR^{\otimes n})_i \operatorname{Tr} M_j E(\rho^{\otimes n})_k \sigma^{\otimes n} = \operatorname{Tr} IR_i^{\otimes n} E(\rho^{\otimes n})_k \sigma^{\otimes n},$$

for states ρ, σ and a PVM $M \in Ir^{\otimes n}$. The number $\#(M/IR^{\otimes n})_i$ corresponds to the number of equivalent irreducible representations in the representation $\pi_{\mathrm{GL}(\mathcal{H})}^{\otimes n}$. Therefore we obtain

$$D_{IR^{\otimes n} \times E(\rho^{\otimes n})}(\sigma^{\otimes n} \| \rho^{\otimes n}) = D_{M \times E(\rho^{\otimes n})}(\sigma^{\otimes n} \| \rho^{\otimes n}). \tag{10}$$

4 Proof of Main Theorem

First we will prove Theorem 2 in the case of that the dimension of $\mathcal{H}$ is finite number k. Let ρ be a state on $\mathcal{H}$. From Theorem 3, Lemma 3 and the preceding discussion, we obtain the following fact. For a PVM $E^n \in Ir^{\otimes n}$, the PVM $M^n := E^n \times E(\rho^{\otimes n})$ satisfies:

$$\frac{D_{M_n}(\sigma^{\otimes n} \| \rho^{\otimes n})}{n} \leq D(\sigma \| \rho) \leq \frac{D_{M_n}(\sigma^{\otimes n} \| \rho^{\otimes n})}{n} + (k-1)\frac{\log(n+1)}{n} \ \forall \sigma. \tag{11}$$

Therefore we obtain

$$\frac{D_{M_n}(\sigma^{\otimes n} \| \rho^{\otimes n})}{n} \to D(\sigma \| \rho) \text{ as } n \to \infty \text{ uniformally for } \sigma. \tag{12}$$

From (10), the PVM $IR^{\otimes n} \times E(\rho^{\otimes n})$ satisfies (11) and (12). We get (5) in the finite-dimensional case. In spin 1/2 system, the PVM $IR^{\otimes n}$ corresponds to the measurement of the total momentum, and $E(\rho^{\otimes n})$ does to the one of the momentum of the direction specified by ρ. These obsarvables are commutative with one another. Next, we consider the infinite-dimensional case. Let $\mathcal{B}(\mathcal{H})$ be the set of bounded operators on $\mathcal{H}$, and $\mathcal{B}(\mathcal{H})^{\otimes n}$ be $\underbrace{\mathcal{B}(\mathcal{H}) \otimes \cdots \otimes \mathcal{B}(\mathcal{H})}_{n}$. According [6], from the separability of $\mathcal{H}$, there exists a finite-dimensional approximation of $\mathcal{H}$. i.e. a sequence $\{\alpha_n : \mathcal{B}(\mathcal{H}_n) \to \mathcal{B}(\mathcal{H})\}$ of unitpreserving completely positive maps such that $\mathcal{H}_n$ is finite-dimensional and

$$\lim_{n \to \infty} D(\alpha_n^*(\sigma) \| \alpha_n^*(\rho)) = D(\sigma \| \rho) \tag{13}$$

for any states σ, ρ on $\mathcal{H}$ such that $\mu\rho \leq \sigma \leq \lambda\rho$ for some positive real numbers μ, λ. From (12), for any positive integer n there exists a pair (l_n, M'_n) of an integer and a PVM on $\mathcal{H}_n^{\otimes l_n}$ such that

$$D(\alpha_n^*(\sigma) \| \alpha_n^*(\rho)) - \frac{D_{M'_n}\left((\alpha_n^*(\sigma))^{\otimes l_n} \middle\| (\alpha_n^*(\rho))^{\otimes l_n}\right)}{l_n} < \frac{1}{n}. \tag{14}$$

The completely positive map $\alpha_n^{\otimes l}$ from $\mathcal{B}(\mathcal{H}_n)^{\otimes l}$ to $\mathcal{B}(\mathcal{H})^{\otimes l}$ is defined as $\alpha_n^{\otimes l}(A_1 \otimes A_2 \otimes \cdots \otimes A_l) = \alpha_n(A_1) \otimes \alpha_n(A_2) \otimes \cdots \otimes \alpha_n(A_l)$ for $\forall A_i \in \mathcal{B}(\mathcal{H})$. Therefore we have $\left(\alpha_n^{\otimes l}\right)^* (\sigma^{\otimes l}) = \alpha_n^*(\sigma)^{\otimes l}$.

Let M_n be $\alpha_n^{\otimes l_n}(M_n')$, then from (13)(14) we get

$$\begin{aligned}
\frac{D_{M_n}(\sigma^{\otimes l_n}\|\rho^{\otimes l_n})}{l_n} &= \frac{D_{M_n'}\left(\left(\alpha_n^{\otimes l_n}\right)^*\left(\sigma^{\otimes l_n}\right)\middle\|\left(\alpha_n^{\otimes l_n}\right)^*\left(\rho^{\otimes l_n}\right)\right)}{l_n} \\
&= \frac{D_{M_n'}\left(\alpha_n^*(\sigma)^{\otimes l_n}\middle\|\alpha_n^*(\rho)^{\otimes l_n}\right)}{l_n} \\
&> D\left(\alpha_n^*(\sigma)\|\alpha_n^*(\rho)\right)+\frac{1}{n} \\
&\to D(\sigma\|\rho) \text{ as } n\to\infty.
\end{aligned}$$

Therefore, we obtain Theorem 2. Note that such a POVM M_n is independent of σ.

Conclusions

It was proved that the quantum relative entropy $D(\sigma\|\rho)$ is attained by the sequence of Kullback-Leibler divergences given by a certain sequence of POVMs which is independent of σ. This formula is thought to be important for the quantum asymptotic detection and the quantum asymptotic estimation. About the quantum asymptotic estimation, see [9]. The realization of the sequence of measurements are left for future study. In spin 1/2 system, it is enough to simultaneously measure the total momentum and the momentum of the direction specified by ρ.

Acknowledgments

The author wishes to thank Prof. D. Petz for essential suggestions about the extension in the infinite-dimensional case. He wishes to thank Dr. A. Fujiwara and Dr. M. Ishii for several discussions on this topic.

References

[1] S. Kullback and R. A. Leibler, Ann. Math. Statist. **22**, 79-86 (1951).

[2] H. Umegaki, Kodai Math. Sem. Rep. **14**, 59 (1962).

[3] C. W. Helstrom, *Quantum Detection and Estimation Theory,* (Academic Press, New York, 1976).

[4] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory,* (North_Holland, Amsterdam, 1982).

[5] A. Uhlmann, Commun. Math. Phys. **54**, 21 (1977).

[6] M. Ohya and D. Petz, *Qunatum Entropy and Its Use,* (Springer, Berlin, 1993).

[7] F. Hiai and D. Petz, Commun. Math. Phys. **143**, 99-114 (1991).

[8] D. Petz, J. Funct. Anal. **120**, 82-97 (1994).

[9] M. Hayashi, J. Phys. A, **31**, 4633-4655 (1998).

[10] R. Goodman and N. Wallch, *Representations and Invariants of the Classical Groups,* (Cambrige University Press, 1998).